

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

HARRIS CORPORATION,

Plaintiff,

vs.

HUAWEI DEVICE USA, INC.
HUAWEI DEVICE CO., LTD.,
HUAWEI TECHNOLOGIES USA INC.,
HUAWEI TECHNOLOGIES CO. LTD., AND
HUAWEI DEVICE (SHENZHEN) CO., LTD.,

Defendants.

No. 2:18-cv-00439-JRG

Jury Trial Demanded

**DEFENDANTS' REPLY IN SUPPORT OF RULE
12(b)(6) MOTION TO DISMISS AMENDED COMPLAINT FOR
FAILURE TO STATE A CLAIM UNDER 35 U.S.C. § 101**

TABLE OF CONTENTS

	<u>PAGE</u>
I. INTRODUCTION	1
II. UNLIKE <i>DDR</i> , NO CHALLENGED CLAIM “OVERRIDES” THE ROUTINE, CONVENTIONAL USE OF THE CLAIMED COMPONENTS/COMBINATIONS	2
III. HARRIS HAS FAILED TO REBUT HUAWEI’S SHOWING THAT THE CLAIMS IDENTIFIED IN THE COMPLAINT ARE REPRESENTATIVE.....	3
IV. THE CLAIMS OF THE ASSERTED PATENTS ARE NOT PATENT ELIGIBLE	4
A. The Claims of the ’678 and ’690 Network Intrusion Detection Patents Do Not Address a Problem Unique to Computer Networking and Do Not Include any Inventive Concept, as the Specifications’ Admissions Confirm	4
B. The Claims of the ’227 Color Coded Map Patent Do Not Purport to Improve the Operation of a Wireless Network, and the Specification Admits that the Only Allegedly Inventive Concept Harris Points to Was Conventional.....	5
C. The Claims of the ’986 Scheduling Patent Apply Age-Old Techniques to a Field of Use, Using Only Functional Language Devoid of Inventive Concept	7
D. The ’426 Claims Merely Apply Conventional Route Finding and Selection Techniques to a Field of Use (Networks with Multiple Frequencies)	8
E. The Claims of the ’537 Status Transmission Patent Do Not Address a Problem Unique to Networking and Recite Only Conventional Components Performing Routine Functions	9
F. The Claims of the ’572 Patent Do Not Purport to Improve Upon Cryptography and Recite No Inventive Concept, as the Specification’s Admissions Confirm	11

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Alice Corp. Pty. Ltd. v. CLS Bank Int’l</i> , 573 U.S. 208 (2014).....	<i>passim</i>
<i>Ancora Techs., Inc. v. HTC Am., Inc.</i> , 908 F.3d 1343 (Fed. Cir. 2018).....	4, 11, 12
<i>Audatex N. Am., Inc. v. Mitchell Int’l, Inc.</i> , 703 F. App’x 986 (Fed. Cir. 2017)	10
<i>Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat’l Ass’n</i> , 776 F.3d 1343 (Fed. Cir. 2014).....	3
<i>Data Engine Techs. LLC v. Google LLC</i> , 906 F.3d 999 (Fed. Cir. 2018).....	6
<i>DDR Holdings, LLC v. Hotels.com, L.P.</i> , 773 F.3d 1245 (Fed. Cir. 2014).....	1, 2, 9
<i>Electric Power Group, LLC v. Alstom S.A.</i> , 830 F.3d 1350 (Fed. Cir. 2016).....	5
<i>FairWarning IP, LLC v. Iatric Sys., Inc.</i> , 839 F.3d 1089 (Fed. Cir. 2016).....	4
<i>Finjan, Inc. v. Blue Coat Sys., Inc.</i> , 879 F.3d 1299 (Fed. Cir. 2018).....	4, 6
<i>Huawei Techs. Co. Ltd. v. T-Mobile US, Inc.</i> , No. 2:16-CV-00052-JRG-RSP, 2017 WL 4118383 (E.D. Tex. Aug. 29, 2017)	1, 13, 14
<i>Intellectual Ventures I LLC v. Capital One Bank</i> , 792 F.3d 1363 (Fed. Cir. 2015).....	10
<i>Intellectual Ventures I LLC v. J. Crew Grp., Inc.</i> , No. 6:16-CV-196-JRG, 2016 WL 4591794 (E.D. Tex. Aug. 24, 2016).....	3
<i>Intellectual Ventures I LLC v. T-Mobile USA, Inc.</i> , No. 2:17-CV-00577-JRG, 2018 WL 6584486 (E.D. Tex. Sept. 4, 2018)	7
<i>Intellectual Ventures II LLC v. Sprint Spectrum, L.P.</i> , No. 2:17-CV-00661-JRG, 2018 WL 6804804 (E.D. Tex. Sept. 24, 2018)	3

<i>Interval Licensing LLC v. AOL, Inc.</i> , 896 F.3d 1335 (Fed. Cir. 2018).....	7
<i>Paone v. Broadcom Corp.</i> , No. 15 Civ. 0596, 2015 WL 4988279 (E.D.N.Y. Aug. 19, 2015).....	11
<i>Personalized Media Commc’ns, LLC v. Apple Inc.</i> , No. 2:15-cv-1366-JRG-RSP, 2016 WL 5719701 (E.D. Tex. Sept. 13, 2016).....	11
<i>Realtime Data, LLC v. Carbonite, Inc.</i> , No. 6:17-cv-00121, 2017 WL 4693969 (E.D. Tex. Sept. 210, 2017).....	11
<i>Sycamore IP Holdings LLC v. AT&T Corp.</i> , 294 F. Supp. 3d 620 (E.D. Tex. 2018).....	11
<i>Two-Way Media Ltd. v. Comcast Cable Commc’ns</i> LLC, 874 F.3d 1329 (Fed. Cir. 2017).....	7, 9, 10
<i>Umbanet, Inc. v. Epsilon Data Mgmt., LLC</i> , 263 F. Supp. 3d 647 (E.D. Tex. 2017).....	1, 9

TABLE OF DEFINITIONS

Term	Definition
Huawei	Defendants Huawei Device USA, Inc., Huawei Device Co., Ltd., Huawei Technologies USA Inc., Huawei Technologies Co. Ltd., and Huawei Device (Shenzen) Co., Ltd.
Harris	Plaintiff Harris Corporation
'678 patent	U.S. Patent No. 7,224,678 (attached as Exhibit A)
'690 patent	U.S. Patent No. 7,327,690 (attached as Exhibit B)
'227 patent	U.S. Patent No. 6,535,227 (attached as Exhibit C)
'986 patent	U.S. Patent No. 6,958,986 (attached as Exhibit D)
'426 patent	U.S. Patent No. 7,027,426 (attached as Exhibit E)
'537 patent	U.S. Patent No. 6,980,537 (attached as Exhibit F)
'572 patent	U.S. Patent No. 7,440,572 (attached as Exhibit G)
Asserted Patents	The '678, '690, '227, '986, '426, '537, and '572 patents
Challenged Claims	All claims of the Asserted Patents

NB: All emphases added and citations omitted unless otherwise noted.

I. INTRODUCTION

As shown in Huawei’s Motion, the Challenged Claims are directed to ideas the Federal Circuit already has found to be impermissibly abstract. Harris’s Response does not dispute that the claims are directed to those abstract ideas. Instead, Harris’s principal argument at *Alice* step one is that the claims are not abstract because they address problems in the field of computer networks; but that is not the test. Far from being “necessarily rooted in computer technology in order to overcome a problem *specifically* arising in the realm of computer networks,” *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014), here the claims are directed to problems that have long existed outside of the realm of computer networks—as Huawei’s unrebutted “real world” analogies demonstrate. *Cf. Huawei Techs. Co. Ltd. v. T-Mobile US, Inc.*, No. 2:16-CV-00052-JRG-RSP, 2017 WL 4118383, at *3 (E.D. Tex. Aug. 29, 2017) (finding patentable claims “directed to a particular technical problem that *only* exists in wireless communication networks”). For example, the problems Harris identifies of detecting intruders, mapping network vulnerabilities, scheduling times for communication, determining routes, and encrypting/encoding data, are not unique to computer networking. Merely limiting the application of these abstract concepts to the field of computer networking, as Harris argues, cannot save the claims. *See, e.g., Umbanet, Inc. v. Epsilon Data Mgmt., LLC*, 263 F. Supp. 3d 647, 653 (E.D. Tex. 2017), *aff’d*, 745 F. App’x 168 (Fed. Cir. 2018) (Gilstrap, J.) (“Taking a generally abstract idea, such as enabling selective access to a message, and limiting it to an ‘email client’ alters the ‘field of use,’ but it cannot ‘render an otherwise abstract concept any less abstract.’”).

Harris’s step two arguments fare no better. First, Harris fails to adhere to the *Alice* requirement that in step two the Court must first remove the abstract idea from the claim, and then “determine whether the *additional* elements” “‘transform the nature of the claim’ into a patent-

eligible application”—focusing on “What *else* is there in the claims” beyond the abstract idea. *Alice Corp. Pty. Ltd. v. CLS Bank Int’l*, 573 U.S. 208, 217 (2014). Instead, Harris repeatedly argues that the abstract idea itself is inventive—a notion roundly rejected by the controlling cases. Second, Harris offers little or no response to Huawei’s showing—based on specification admissions and prior Federal Circuit decisions—that such “additional elements” of Harris’s claims are entirely routine and conventional, individually and as an ordered combination. And while Harris rightly observes that an “ordered combination” *can* be inventive, Harris does not identify a single “ordered combination” claimed here that it alleges *is* inventive—because none even arguably is. Most telling of all, Harris never contends that any Challenged Claim “overrides” the routine and conventional use of the claimed components/combinations. *DDR*, 773 F.3d at 1258.

II. UNLIKE *DDR*, NO CHALLENGED CLAIM “OVERRIDES” THE ROUTINE, CONVENTIONAL USE OF THE CLAIMED COMPONENTS/COMBINATIONS

Harris’s reliance on *DDR* and its progeny is misplaced. *DDR* is not only distinguishable, but the differences between the claims there and here underscore the ineligibility of the Challenged Claims. *DDR* affirmed the patentability of the claims because they were directed to an “override” of the way computer systems normally operated when an end-user clicked on an advertiser’s hyperlink. 773 F.3d at 1258-59 (“a result that overrides the routine and conventional sequence of events ordinarily triggered by the click of a hyperlink”). Under the claimed invention, “[i]nstead of the computer network operating in its normal, expected manner by sending the website visitor to the third-party website ...,” the user was taken to a hybrid page that retained the look and feel of the original web page, but allowed the user to purchase the advertised product. *Id.*

The challenged claims here effect no such “override.” To the contrary, they do the exact opposite, reciting only conventional components performing the same functionality those components have always performed. The ’678 and ’690 network intrusion detection patents recite

generic networking components to monitor the transmission of data. The '227 color coded map patent admits that the purported invention can be practiced with off-the-shelf software running on a generic PC in its usual manner. The '986, '426, and '537 patents recite conventional components, such as transceivers and controllers, that perform their expected, routine functions of sending, receiving, and/or directing information. And the '572 cryptography patent recites a “cryptography circuit” for performing the conventional function of encrypting/decrypting data.

III. HARRIS HAS FAILED TO REBUT HUAWEI'S SHOWING THAT THE CLAIMS IDENTIFIED IN THE COMPLAINT ARE REPRESENTATIVE

Not only are the Motion's representative claims the only claims identified in the Amended Complaint (Dkt. 13), Huawei's Motion demonstrates that the remaining Challenged Claims are “substantially similar and linked to the same abstract idea” as the representative claims using well-supported analyses that address every single Challenged Claim. *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat'l Ass'n*, 776 F.3d 1343, 1348 (Fed. Cir. 2014). Unlike the bare, conclusory footnote in *Sprint*, Huawei's Motion discusses the differences and additional elements recited in each claim. *Compare Intellectual Ventures II LLC v. Sprint Spectrum, L.P.*, No. 2:17-CV-00661-JRG, 2018 WL 6804804, at *2-3 (E.D. Tex. Sept. 24, 2018), with Mot. 6-7 & n. 4, 12, 17, 19-22, 31. Asserted claims are often held representative of the other patent claims for § 101 purposes, and Huawei's motion shows why that is appropriate here. *See Intellectual Ventures I LLC v. J. Crew Grp., Inc.*, No. 6:16-CV-196-JRG, 2016 WL 4591794, at *4 (E.D. Tex. Aug. 24, 2016) (finding one claim to be representative of 50).

Harris utterly fails to rebut Huawei's showing of representativeness. Indeed, the *only* non-asserted claim that Harris argues to be 101-eligible for independent reasons is '572 dependent claim 7—and that argument backfires. That claim, which adds only a “protection circuit,” recited only in functional terms for “protect[ing] against transmission of unencrypted data,” reinforces the

conclusion that the ‘572 claims are directed to the abstract idea of encrypting and decrypting data.

IV. THE CLAIMS OF THE ASSERTED PATENTS ARE NOT PATENT ELIGIBLE

A. The Claims of the ‘678 and ‘690 Network Intrusion Detection Patents Do Not Address a Problem Unique to Computer Networking and Do Not Include any Inventive Concept, as the Specifications’ Admissions Confirm

The ‘678 and ‘690 claims are directed to monitoring communications to detect suspicious behavior and generating an alert—a concept that the Federal Circuit has deemed abstract, and that can be performed with pen and paper. Mot. 7-9. Harris does not dispute these points. Nor does it contend that detecting intrusions is a problem unique to computer networks.

Notably, the claims do not say *how* to do the recited monitoring or detection—they merely recite the *idea* of doing that monitoring/detection, which is not patentable. See *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299, 1305 (Fed. Cir. 2018) (“[A] result, even an innovative result, is not itself patentable.”).¹ Like the impermissibly abstract claims in *FairWarning* that recite particular rules (*e.g.*, accesses in excess of a specific volume, accesses during a predetermined time interval, accesses by a specific user), the ‘678 and ‘690 claims include the same level of specificity and are unpatentable. *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1094 (Fed. Cir. 2016).

Despite Harris’s representations, even the specification excerpts it identifies are silent on *how* to perform the claimed monitoring and detection. For example, Figure 20 of the ‘690 does not explain *how* to monitor for or detect collisions of the same MAC address.² Indeed, the figures

¹ The claims here are unlike *Finjan*’s claims to a “behavior-based virus scan” directed to a specific improvement in computer functionality, reciting “*specific* steps ... that accomplish the desired result,” *id.* at 1304-06, and unlike those in *Ancora*, where the claimed method “*specifically* identifies *how* th[e] functionality improvement is effectuated in an assertedly *unexpected* way.” *Ancora Techs., Inc. v. HTC Am., Inc.*, 908 F.3d 1343, 1348 (Fed. Cir. 2018).

² Nor do Figures 4 or 14 in the ‘678 patent explain *how* to “detect contention-free mode operation outside of a CFP,” Figures 3 and 13 explain *how* to detect an “illegal NAV value,” or Figures 2 and 12 explain *how* to “detect failed attempts to authenticate MAC addresses.” Mot. 14.

and the corresponding specification disclosures identify only what to monitor and detect—not how to do it. *See, e.g.*, ’678 and ’690 Figs. 1-10 (see policing node/station), 11-21 (see monitor loop).

Far from excising the abstract idea from the claim at step two as required, the *only* allegedly inventive aspect Harris points to is the *abstract idea* of monitoring certain information to detect intrusions. Opp. 16. If Harris first removed the abstract idea from the claim before looking at “what else” there is, Harris would admit the claim recites nothing that would transform it into a patent-eligible application of the abstract idea. *Alice*, 573 U.S. at 217. Regardless, Harris does not contest that the information monitored/detected in the claims was conventionally transmitted pursuant to the existing 802.11 standard, or pretend it invented—let alone claimed—a new way of monitoring that existing information. Harris also does not contend that the claims are inventive as an ordered combination, which is unsurprising since they require the entirely ordinary steps of first monitoring for information and then generating an alert if that information is detected.

B. The Claims of the ’227 Color Coded Map Patent Do Not Purport to Improve the Operation of a Wireless Network, and the Specification Admits that the Only Allegedly Inventive Concept Harris Points to Was Conventional

The ’227 claims are directed to the abstract idea of collecting information, analyzing it, and displaying certain results of that collection and analysis, analogous to the power grid network map claims held to be unpatentable in *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016)—a showing Harris was unable to rebut.³ *See* Mot. 12-13. In addition, Harris does not contest the specification’s admissions that the claimed system can be practiced with off-the-shelf software running on a standard PC. Mot. 13.

Harris contends that, in describing the abstract idea, Huawei ignores the specification’s discussion of improvements in establishing a “security posture,” but Harris ignores that the Court

³ Harris’s reliance on “specific improved structures or techniques” to distinguish *Electric Power* similarly fails as it does not identify any such distinguishing structures or techniques. Opp. 20.

must examine the patent’s “‘**claimed**’ advance’ to determine whether the claims are directed to an abstract idea.” *Finjan*, 879 F.3d at 1303. While the claims recite the establishment of a “security posture,” the specification acknowledges that security engineers had long been establishing a “security posture” for their networks through various means. ’986 at 2:35-44. And the claims do not require any specific means of establishing a security posture except by “correlating” a database with “any” data obtained from programs. *Id.* 16:20-26, 16:49-56. The requirement that information be correlated, a process that can be done manually and mentally, does not save the claims from abstractness. *See* Mot. 13.

Harris’s heavy reliance on *Data Engine Techs. LLC v. Google LLC* also does not save the claims from being abstract. There, the claims required “a **specific** interface and implementation ... using techniques **unique** to computers,” and the improvement of the claims “allowed computers, **for the first time**, to provide rapid access to and processing of information in different spreadsheets” 906 F.3d 999, 1008-09 (Fed. Cir. 2018). No similar factors exist here. The claims here do not require a specific interface and implementation using techniques unique to computers (color coding certainly is not unique), and the specification admits that the network map may be created using preexisting HP software. ’277 at 5:50-54, 6:34-38.

Harris also does not identify any supposed inventive concept sufficient to transform the ’227 claims into eligible subject matter. The specification admits that determining or establishing a security posture was conventional activity, *id.* at 2:31-37, and that variations of GUI structures, such as the claimed vulnerability profile that merely depicts a radio button selection of low, medium, or high (*see* ’227 Fig. 8B), is not an inventive concept, *id.* at 8:36-39, 8:47-49. Likewise, using a database for “correlating” information, *id.* at 16:20-27, is not inventive. The specification is clear that vulnerability programs used in connection with the alleged invention are “standard

[off-the-shelf] programs known by security engineers, and include HP Open View”—a program the specification admits provides for automatic network discovery and graphically depicts network topology. *Id.* at 5:50-54, 6:34-38; see Mot. 11-12. And despite Harris’s conclusory assertion that “each of the claims contains an inventive concept as an ordered combination,” it identifies no allegedly inventive “combination”—and so fails to rebut Huawei’s showing. Opp. 21-22.

C. The Claims of the ’986 Scheduling Patent Apply Age-Old Techniques to a Field of Use, Using Only Functional Language Devoid of Inventive Concept

Harris does not dispute that the ’986 claims are directed to adjusting a schedule based on acquired information. Instead, Harris erects the strawman argument that not *all* network routing and scheduling patents are *per se* abstract. Opp. 24. While that may be true, it is irrelevant because the claims *here* are directed to the foregoing idea, which indisputably is abstract. *Interval Licensing LLC v. AOL, Inc.*, 896 F.3d 1335, 1346 (Fed. Cir. 2018). See Mot. 22.

Harris primarily relies on the distinguishable *Intellectual Ventures I LLC v. T-Mobile USA, Inc.*, No. 2:17-CV-00577-JRG, 2018 WL 6584486, at *2-3 (E.D. Tex. Sept. 4, 2018). There, the claim was “directed to a technical solution to a technical problem” and “explicit in its solution to these problems.” *Id.* at *3. Here, the problem of scheduling time slots for communication is not technical or unique to wireless communications, existing instead in many contexts outside of computer networks. Further, the ’986 claims do not provide a technical solution, reciting only conventional components performing only routine tasks (controller for scheduling and determining) and do not limit *how* technologically to perform the claimed steps of scheduling time slots or determining link utilization metrics. As Harris notes, the claims just say to do it. Opp. 23 (quoting claim 1: “determining respective link utilization metrics . . .”).

Harris’s attempts to distinguish *Interval Licensing*, *Two-Way*, and *Affinity Labs.*, also fail. As in each of those cases, this Court may “look[] for, but simply [will] not find on the facts, the

‘specific improvement to the way computers [or other technologies] operate,’” Opp. 25, particularly here, where the scheduling could be done by pen and paper.

Despite alleging that Huawei has ignored key elements and the claims as ordered combinations for *Alice* step two, Harris points to no combinations and only two elements. But these elements, link utilization metrics and time slot allocations, do not transform the claims into patentable applications of the abstract idea. First, those are merely elements of the abstract idea to which the claim is directed (adjusting a schedule based on acquired information), which are improper to consider at step two. Second, the specification admits that conventional communication links are established by scheduling time slots, ’986 at 1:24-64, and link utilization metrics merely measure data that has been conveyed, *id.* at 4:34-41. Neither suffices. *See* Mot. 16-17. Finally, both elements can exist in one’s mind alone, thus being insufficient “to ‘transform’ the claimed abstract idea into a patent-eligible application.” *Alice*, 573 U.S. at 217-18.

D. The ’426 Claims Merely Apply Conventional Route Finding and Selection Techniques to a Field of Use (Networks with Multiple Frequencies)

The ’426 claims contain the basic steps, and are directed to the abstract idea, of sending route finding requests and selecting a route. Finding and selecting a route from one point to another is not a problem that arises “only” in wireless networks. And even if it were, Harris cannot seriously contend the claims present a technological solution where Harris does not contest, as Huawei demonstrates in its Motion, that the route finding process set forth in the claims was known and conventional. Mot. 24 & n.13. The mere application of these techniques to “electrically separate channels” does not alter the analysis. Electrically separate channels refer merely to channels with, for example, different frequencies. Taking conventional route finding techniques from a single frequency network and using them instead in a multifrequency network may “alter[] the ‘field of use, . . . [but] it cannot ‘render an otherwise abstract concept any less abstract.’”

Umbanet, 263 F. Supp. 3d at 653 (quoting *Intellectual Ventures*, 850 F.3d at 1340).

For these reasons, Harris misplaces its reliance on *SRI International, Inc. v. Cisco Systems, Inc.* Opp. 31. The *SRI* claims “actually prevent the normal, expected operation of a conventional computer network.” No. 2017-2223, 2019 WL 1271160, at *4 (Fed. Cir. Mar. 20, 2019) (noting that, like in *DDR*, the claims override the conventional sequence of events). Here, in contrast, the claimed route finding was admittedly conventional—there is no “override” of a wireless network’s conventional operation.

Similarly, in step two, Harris errs in relying on sending a route request and selecting a route as being allegedly inventive, both because the specification admits those steps are conventional and because *Alice* step two looks only at what remains *after* the abstract idea is removed. While the claims apply those conventional techniques to networks with electrically separate channels, such field of use limitations are legally insufficient. Tellingly, Harris does not dispute that the ’426 claims and specification are silent on *how* to establish a network of electrically separate channels or specifically *how* to send route finding requests over each of a plurality of electrically separate channels— instead just saying “do it.” See Mot. 18, 24-25. As in *Affinity Labs of Texas, LLC v. Amazon.com, Inc.*, “[t]he features set forth in the claims are described and claimed generically rather than with the specificity necessary to show how those components provide a concrete solution to the problem addressed by the patent.” 838 F.3d 1253, 1271 (Fed. Cir. 2016).

E. The Claims of the ’537 Status Transmission Patent Do Not Address a Problem Unique to Networking and Recite Only Conventional Components Performing Routine Functions

Harris does not dispute that the ’537 claims are, as Huawei’s Motion demonstrated, indistinguishable from and directed to the same abstract idea as the claims in *Two-Way Media*— sending, directing, and monitoring information. Instead, Harris tries to downplay the significance of that case, contending that Huawei cites it only because that case also involves the transmission

of data. But the parallels run far deeper. Both here and there, the representative claims “recite[] a method for routing information using result-based functional language” and “require[] the functional results [of the claimed steps] . . . , but do[] not sufficiently describe how to achieve these results in a non-abstract way.” *Two-Way Media Ltd. v. Comcast Cable Commc’ns LLC*, 874 F.3d 1329, 1337 (Fed. Cir. 2017). ’537 claim 30 recites: the transmission of information, but not how; adjusting those transmissions, but not how (only that it is “in response to” detecting modifications in other information, and again the claim is silent on how the detecting occurs); and determining certain information (status of a communication unit), but not how.

And contrary to Harris’s suggestion, there is nothing inventive about using conventional computer networks to perform an abstract idea more efficiently. *Intellectual Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363, 1370 (Fed. Cir. 2015) (“[M]erely adding computer functionality to increase the speed or efficiency of the process does not confer patent eligibility on an otherwise abstract idea.”); *see also Audatex N. Am., Inc. v. Mitchell Int’l, Inc.*, 703 F. App’x 986, 990 (Fed. Cir. 2017), *cert. denied*, 138 S. Ct. 1694 (2018) (finding ineligible under § 101 claims that “neither improve the technological infrastructure nor provide solutions to challenges particular to the Internet” but “[r]ather . . . add computer functionality and recite use of the Internet to increase the speed and efficiency of an abstract process”). The ’537 claims likewise recite the use of conventional computer networks, but do not improve them.

Similarly, Harris’s arguments do not rebut Huawei’s showing that, once the abstract idea is removed, there is no inventive concept to save the claims from invalidity. Tellingly, Harris does not dispute the patent’s extensive admissions that the claims can be performed using routine, conventional components. *See* ’537 patent, 21:18-23:4 and Mot. 27-28. Instead, Harris points to just two allegedly inventive concepts in the claims, but neither withstands scrutiny. Opp. 28. First,

Harris points to alleged “techniques” for sending and adjusting information, but as noted above, the claims are devoid of any limitation on **how** a unit status message is sent or **how** the time interval between transmissions is adjusted. In any event, sending and directing information is entirely routine. *See* Mot. 28-29. Second, Harris contends that the formation of a third network tier is inventive, but the specification admits in the “Background” section that hierarchical network architectures with “plural tiers” were well-known. ’537 at 1:57-60. There is nothing inventive in the claims sufficient to overcome their abstractness.

F. The Claims of the ’572 Patent Do Not Purport to Improve Upon Cryptography and Recite No Inventive Concept, as the Specification’s Admissions Confirm

Harris does not dispute that the claims of the ’572 patent are directed to encrypting and decrypting data, nor does it contest that encrypting and decrypting data is an abstract idea. Harris also does not meaningfully distinguish the analogous case cites in Huawei’s Motion. Instead, Harris argues that not **all** claims that involve encoding/decoding necessarily are abstract—an unremarkable proposition—and cites to cases that affirmed the patentability of claims to specific compression or encryption techniques. Not only are the claims in those cases distinguishable, but also their differences from the claims here underscore why the latter are ineligible.⁴ For example, the representative claim in *Ancora* had the “specificity required to transform [the] claim from one claiming only a result to one claiming a way of achieving it,” because among other things, the claim “moves a software-verification structure to a BIOS location not previously used for this

⁴ *See Realtime Data, LLC v. Carbonite, Inc.*, No. 6:17-cv-00121, 2017 WL 4693969, at *7 (E.D. Tex. Sept. 210, 2017) (“**specific compression techniques** to achieve an increase in data storage and retrieval bandwidth in a memory device”); *Sycamore IP Holdings LLC v. AT&T Corp.*, 294 F. Supp. 3d 620, 652-53 (E.D. Tex. 2018) (specific compression protocol); *Personalized Media Commc’ns, LLC v. Apple Inc.*, No. 2:15-cv-1366-JRG-RSP, 2016 WL 5719701, at *5-6 (E.D. Tex. Sept. 13, 2016) (“[T]he claim and the specification show that using a ‘control signal’ to control decryption improves the way in which ‘encrypted digital programming’ is delivered.”); *Paone v. Broadcom Corp.*, No. 15 Civ. 0596, 2015 WL 4988279, at *8 (E.D.N.Y. Aug. 19, 2015) (“encrypting digital information using a symmetric key block cipher with dynamic keys”).

computer-security purpose and alters how the function is performed.” 908 F.3d at 1349-50. Here, in contrast to the “specific improvements to existing encryption technology” in those cases, Opp. 34, there can be no dispute that the ’572 claims to an encryption circuit for encrypting data do not improve upon exiting encryption technology. Harris’s own description of the alleged invention reinforces the abstract nature of the claims here. The problem the patent addresses, according to Harris, is one where “bad actors observe” unprotected information. Opp. 31-32. Shielding information from prying eyes is not a problem unique to computer networks.

At *Alice* step two, Harris does not dispute that the claimed invention encompasses an off-the-shelf cryptography circuit—reinforcing that the claims are not directed to any advancement in cryptography. Further belying Harris’s argument that “the *claimed* cryptography circuit” is unconventional, Opp. 35, the claims recite that element using purely functional terms, where those functions—encrypting and decrypting—are the routine functions of any cryptography circuit.

Harris’s remaining step two arguments are equally unavailing. It argues that encrypting address and data information is unconventional and therefore saves the claim. Opp. 35. But the claimed **idea** of encrypting both address and data information is abstract, and *Alice* step two requires examining “what else is there.” 573 U.S. at 217. Lastly, Harris claims that the addition of encrypting bits was inventive, despite the specification’s admission that it was a known technique. *See* Mot. 33. Harris attempts to contort the words of the specification by asserting that the addition of encrypting bits “requires” transmission over an extended time. Opp. 35. Not only does the specification not say that an extended transmission time scheme is required, it expressly states that “other schemes” may be used, ’572 at 5:50-52. Further, and critically, the claims are not limited to one of those specific transmission schemes. Once the abstract idea is teased out, nothing inventive remains and the claims fail under § 101.

Dated: March 29, 2019

/s/ Melissa R. Smith

Melissa R. Smith
GILLAM & SMITH, LLP
TX State Bar No. 24001351
303 S. Washington Ave.
Marshall, Texas 75670
Telephone: (903) 934-8450
Facsimile: (903) 934-9257
melissa@gillamsmithlaw.com

James R. Batchelder
(CA Bar No. 136347)
(Eastern District of Texas Member)
James L. Davis, Jr.
(CA Bar No. 304830)
(Eastern District of Texas Member)
Andrew T. Radsch
(CA Bar No. 303665)
(Eastern District of Texas Member)
Christopher M. Bonny
(CA Bar No. 280554)
(Eastern District of Texas Member)
ROPES & GRAY LLP
1900 University Avenue, 6th Floor
East Palo Alto, CA 94303-2284
Telephone: (650) 617-4000
Facsimile: (650) 617-4090
james.batchelder@ropesgray.com
james.l.davis@ropesgray.com
andrew.radsch@ropesgray.com
christopher.bonny@ropesgray.com

Jolene L. Wang
(NY Bar No. 5462619)
ROPES & GRAY LLP
1211 Avenue of the Americas
New York, NY 10036
(212) 596-9000
(212) 596-9090
jolene.wang@ropesgray.com

Attorneys for Defendants
*HUAWEI DEVICE USA, INC., HUAWEI
DEVICE CO., LTD., HUAWEI
TECHNOLOGIES USA INC., HUAWEI
TECHNOLOGIES CO. LTD.,*

*and HUAWEI DEVICE (SHENZHEN) CO.,
LTD.*

CERTIFICATE OF SERVICE

I hereby certify that counsel of record who are deemed to have consented to electronic service are being served this 29th day of March, 2019, with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3).

/s/ Melissa R. Smith
Melissa Smith

